



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/852,372	05/10/2001	Dale E. Gulick	2000.038300/TT3756	5417
23720	7590	12/15/2004	EXAMINER	
WILLIAMS, MORGAN & AMERSON, P.C. 10333 RICHMOND, SUITE 1100 HOUSTON, TX 77042			POLTORAK, PIOTR	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 12/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/852,372

Applicant(s)

GULICK ET AL.

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 May 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 52 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 52 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 May 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 9/30/2002.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-52 have been examined.

Drawings

2. The drawings are objected to because Fig. 3 as discussed in the specification does not show "computer system 100", and the object 200 in Fig. 3 is not addressed in the specification.
3. Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 6, 16, 26, 31, 37 and 50 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.
5. The phrase “substantially” in claim 16 is not well understood.
6. Claim 6 is not well understood. Claim 6 is dependent on claim 5 which recites the limitation of “a kick-out timer configured to provide an indication to the processor of when the processor to exit the secure mode” which is essentially the same as the limitation of claim 6. However, in the case of claim 6 the “re-initiation timer” is recited in place of “a kick-out timer”. As a result it is not clear whether the “kick-out timer” is the same as “re-initiation timer”. If it is not to be interpreted as the “kick-out timer” the claim language does not allow distinguishing the two from each other.
7. The “indicative of the entry in response to providing the entry” in claim 26 line 25 is not well understood.
8. The “in lieu of data” in claims 11, 31, 37 and 50 is not well understood since any response will contain data.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1, 16, 21, 34, 39 and 40 are rejected under 35 U.S.C. 102(b) as being anticipated by *Takahashi et al.* (U.S. Patent No. 5615263).

As per claim 1 *Takahashi et al.* teach "A secure mode within a dual mode processor is implemented" (*Abstract*) reads on the limitation in claim 1 wherein a processor is configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode.

Takahashi et al. teach primitives which encrypt/decrypt the data (*secure assets*), I/O hardware control circuit and assurance logic (*security hardware*) (*col.2 lines 10-13, col. 3 lines 53-59 and col. 4 lines 29-34*) which read on "security hardware configured to control access to the secured assets dependant upon the operating mode of the processor, wherein the security hardware is configured to allow access to the secure assets in the secure operating mode".

Claims 21, 34, 39 and 40 are substantially equivalent to claim 1; therefore claims 21, 34, 39 and 40 are similarly rejected.

As per claim 16 *Takahashi et al.* teach that in while in secure mode, processing functions execute only the secure primitives in ROM but they still have the ability to access external memory for data (*col.3 lines 53-57*) which reads on the processor being configured to store and retrieve data from the memory in substantially all of the plurality of operating modes.

Art Unit: 2134

10. Claims 1-9, 19, 21-22, 25-28, 32, 34-36, 38-41, 44-47 and 51 are rejected under 35 U.S.C. 102(e) as being anticipated by *Angelo et al.* (U.S. Patent No. 6581162).

As per claim 1 *Angelo et al.* teach "A method for securely managing encryption information in a computer system, having a secure mode of operation and a normal mode of operation" (*col.10 lines. 53-55*) which read on the limitation "a processor configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode".

The limitation "one or more secured assets coupled to the processor" is met by secure memory (*col. 3 lines 12-16*).

Furthermore, *Angelo et al.* teach "storing an encryption algorithm in a secure memory space not accessible to the normal software processes and only accessible by the general processor in the secure mode of operation" (*col. 10 line 66- col. 11 line 2*) and PCI-ISA bridge to allow access to protected resources (*col. 4 lines 56-64*). This reads on "security hardware configured to control access to the secured assets dependant upon the operating mode of the processor, wherein the security hardware is configured to allow access to the secure assets in the secure operating mode".

Claims 21, 34, 39 and 40 are substantially equivalent to claim 1; therefore claims 21, 34, 39 and 40 are similarly rejected.

As per claim 3-4, 25-27, 35, 44-46 *Angelo et al.* teach system management mode (SMM) which is entered upon receipt of a system management interrupt (SMI).

Angelo et al. also teach SMI asserted by either an SMI timer or by a system request

Art Unit: 2134

upon which the entire CPI state is saved in the SMM memory. After the initial processor state is saved, the processor begins executing an SMI handler routine providing security services (*col. 7 line 43- col. 8 line 4*).

The above reads on receiving a request to change the computer system from the first operating mode to the secure operating mode, providing an entry into an initiation register and asserting the control signal indicative of the entry providing a system management interrupt.

As per claims 5-9, 28, 36 and 47 *Angelo et al.* teach timers (*col. 4 line 58*). When the computer system detects a request for secure communications or any event requiring secure entry of encryption information. Control then proceeds to step where appropriate registers in processor are loaded prior to execution of the SMI code (*Fig. 5, col. 9 lines 3-13*). The computer systems don't wait indefinitely for input of the sensitive information like passwords. Timer measuring a time period in which the computer system is in the secure operating mode, and providing a control signal to exit the secure mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time are used complete indefinite sessions.

As per claim 19 *Angelo et al.* teach a battery providing reserve power to the security hardware (*col. 8 lines 23-25*).

Claims 1, 21, 34, 40 are rejected under 35 U.S.C. 102(b) as being anticipated by *Angelo et al.* (*U.S. Patent No. 5748888*).

As per claim 21 *Angelo et al.* teach a method for providing access to secured assets in a computer system, the method including switching the computer system between a first operating mode and a second operating mode where the second operating mode includes a secure operating mode (*col. 2 lines 40-51 and Fig. 2 steps 404-410*). The access to the secured assets is permitted in response to the computer system being in the secure operating mode and restricted when in the first operating mode.

11. Claims 1, 11-13, 15-16, 21, 30, 32-35, 38-39 and 40-41, 44-46, 49, 51-52 are rejected under 35 U.S.C. 102(b) as being anticipated by *Hadfield et al.* (*Lee Hadfield, Dave Hatter, Dave Bixler, "Windows NT Server 4 security handbook", 1997, ISBN: 078971213-x.*)

As per claim 1 *Hadfield et al.* teach that a processor is configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode and secure assets (*e.g. files*) that can only be accessed in the secure mode. Windows NT runs on hardware, the computers which use processors. Each user that accesses any Windows NT Server-based resources first must be validated by the system, and the user is required to enter a valid password before any interactive Windows session is allowed (*pg. 45, User Accounts in a Windows NT Environment*).

Claims 21, 34, 39 and 40 are substantially equivalent to claim 1; therefore claims 21, 34, 39 and 40 are similarly rejected.

Art Unit: 2134

As per claim 15 the limitation "scratchpad RAM, wherein each of the one or more secured assets is configured to access the scratchpad RAM for the storage of data" computers store applications and files accessed by users in (*scratchpad*) RAM.

As per claims 11-13, 30, 49 computer RAM in Windows NT Server stores input and output data in memory banks (*mailbox RAM*), and the input data for the one or more secured assets is addressed to the RAM and the output data is retrieved from an address at the RAM.

Also, as discussed above in reference to claim 1, users don't have access to the system until the log-on sequence allows them to log-on to the system and enter the secure mode. It is inherent to have filters configured not to provide input data to RAM if the processor is not operating in the secure operating mode.

Upon receipt of the access request if the processor is not operating in the secure operating mode (placing an incorrect password and/or user name while attempting to access the system) will result in an error message and denial of access to the system will result in a predetermined response in lieu of data.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2134

12. Claims 17-18, 31, 37 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Hadfield et al.* (Lee Hadfield, Dave Hatter, Dave Bixler, "Windows NT Server 4 security handbook", 1997, ISBN: 078971213-x) in view of the Official Notice.

As per claims 17-18 access locks configured to disable the access filters in an unlocked mode is implicit, otherwise a user would have to log-in to the system each time the user would try to access some files.

Hadfield et al. do not explicitly teach the access filters being configured to provide a predetermined response in lieu of data if the processor is not operating in the secure operating mode.

Official Notice is taken that it is old and well-known to provide a predetermined response in lieu of data upon receipt of an access request to restricted assets.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure the access filters to provide a predetermined response in lieu of data upon receipt of an access request to restricted assets. One of ordinary skill in the art would have been motivated to perform such a modification so that a user would be aware of the failure and take appropriate action (type password again, for example).

As per claims 31, 37 and 50 *Hadfield et al.* do not explicitly teach providing a predetermined response in lieu of data upon receipt of an access request to restricted assets.

Art Unit: 2134

Official Notice is taken that it is old and well-known to provide a predetermined response in lieu of data upon receipt of an access request to restricted assets.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to provide a predetermined response in lieu of data upon receipt of an access request to restricted assets. One of ordinary skill in the art would have been motivated to perform such a modification so that a user would be aware of the failure and take appropriate action (type password again, for example).

13. Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Hadfield et al. (Lee Hadfield, Dave Hatter, Dave Bixler, "Windows NT Server 4 security handbook", 1997, ISBN: 078971213-x) in view of *Heald et al.* (U.S. Patent No. 5272382).

Hadfield et al. teach a system including secured assets and security hardware as discussed above.

Hadfield et al. do not teach a battery wherein the battery provides reserve power to one or more secured assets and to the security hardware.

Heald et al. teach a battery providing reserve power (*Heald et al.*, Abstract and col. 7 lines 8-16).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a battery providing reserve power to *Hadfield et al.*'s system including secured assets and security hardware as taught by *Heald et al.* One of ordinary skill in the art would have been motivated to perform such a modification in

Art Unit: 2134

order to avoid loss of data and damage of secure assets and hardware (*Heald et al.*, col.1 lines 49-52).

14. Claims 24 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Hadfield et al.* (Lee Hadfield, Dave Hatter, Dave Bixler, "Windows NT Server 4 security handbook", 1997, ISBN: 078971213-x.) in view of *Vogt et al.* (U.S. Patent No.6775776).

15. *Hadfield et al.* teach a system as discussed above.

16. *Hadfield et al.* do not explicitly teach a monotonic counter, and wherein permitting access to secured assets include requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter (col. 7 line 66- col. 8 line 2).

17. *Vogt et al.* teach a monotonic counter (*Vogt et al.*, col. 7 line 56-col. 8 line 7) and implicitly teach permitting access to secured assets include requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter.

18. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a monotonic counter wherein permitting access to secured assets include requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter as taught by *Vogt et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent a communication from being recorded and later played back to simulate a legitimate communication (*Vogt et al.*, col. 7 lines 64-66).

19. Claims 23 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Hadfield et al.* (Lee Hadfield, Dave Hatter, Dave Bixler, "Windows NT Server 4 security handbook", 1997, ISBN: 078971213-x.) in view of *Anderson, Jr.* (U.S. Patent No. 5805674).
20. *Hadfield et al.* teach a system as discussed above.
21. *Hadfield et al.* do not teach the secure asset including a random number generator where permitting access to the secured assets includes requesting and receiving a random number from the random number generator.
22. *Anderson, Jr.* teach a random number generator facilitating the random selection of the security phrases which read on requesting and receiving a random number from the random number generator (*Anderson, Jr., col. 7 lines 55-60*).
23. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a random number generator as secure assets to the *Hadfield et al.*'s system in such a way that permitting access to the secured assets would include requesting and receiving the random number as taught by *Anderson, Jr.* One of ordinary skill in the art would have been motivated to perform such a modification in order to increase security (*Anderson, Jr., col. 7 line 55-60*).
24. Claim 2 and 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Hadfield et al.* (Lee Hadfield, Dave Hatter, Dave Bixler, "Windows NT Server 4 security handbook", 1997, ISBN: 078971213-x.) in view of *Aaro et al.* (U.S. Patent No. 6662020) and in view of *Official Notice*.

Art Unit: 2134

25. As per claim 14 *Hadfield et al.* teach inbox mailbox RAM storing input data for the one or more secured assets and an outbox mailbox RAM storing output data from the one or more secured assets as discussed above.
26. *Hadfield et al.* do not teach access filters configured to provide input data or access request to the inbox of the mailbox RAM if the processor is operating in the secure operating mode wherein the access filters are further configured not to provide input data to the inbox of the mailbox RAM if the processor is not operating in the secure operating mode, and wherein the access filters are further configured to provide a predetermined response in lieu of data upon receipt of said access request if the processor is not operating in the secure operating mode.
27. *Aaro et al.* teach a device including a secure memory for storing data directly coupled to the display in the secure mode of operation. The hardwired connections to secure memory in the secure mode ensures that data shown on the display is indeed the data that is processed and signed off in the secure mode of operation (*Abstract*). The secure memory 1 is accessed only by the cryptographic module and the CPU, display and possibly the keypad, or rather its buffer, in the secure mode of operation. In the normal mobile phone mode of operation, access to this secure memory is impossible (*col. 4 lines 55-61*). The above reads on providing input data or access request to the inbox of the mailbox RAM if the processor is operating in the secure operating mode wherein the access filters are further configured not to provide input data to the inbox of the mailbox RAM if the processor

Art Unit: 2134

is not operating in the secure operating mode. The use of access filters configured appropriately so that task can be accomplished is implicit.

28. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to access filters configured to provide input data or access request to the inbox of the mailbox RAM if the processor is operating in the secure operating mode wherein the access filters are further configured not to provide input data to the inbox of the mailbox RAM if the processor is not operating in the secure operating mode as taught by *Aaro et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent malicious programs such as viruses, to gain access to secure memory affecting secure assets (*Aaro et al. col. 2 lines 25-37*).

29. Official Notice is taken that it is old and well-known to provide a predetermined response in lieu of data upon receipt of an access request to restricted assets.

30. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Angelo et al.* (U.S. Patent No. 6581162) in view of *Heald et al.* (U.S. Patent No. 5272382).

31. *Angelo et al.* teach a system including secured assets and security hardware as discussed in paragraph 10.

Angelo et al. do not teach a battery wherein the battery provides reserve power to one or more secured assets and to the security hardware.

32. *Heald et al.* teach a battery providing reserve power (*Heald et al., Abstract and col. 7 lines 8-16*).

33. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a battery providing reserve power to *Angelo et al.*'s system including secured assets and security hardware as taught by *Heald et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid lost of data and damage of secure assets and hardware (*Heald et al.*, col. 1 lines 49-52).

34. Claims 23 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Angelo et al.* (U.S. Patent No. 6581162) in view of *Anderson, Jr.* (U.S. Patent No. 5805674).

35. *Angelo et al.* teach a system as discussed in paragraph 10.

Angelo et al. do not teach secure assets including a random number generator where permitting access to the secured assets includes requesting and receiving a random number from the random number generator.

36. *Anderson, Jr.* teach a random number generator facilitating the random selection of the security phrases which read on requesting and receiving a random number from the random number generator (*Anderson, Jr.*, col. 7 lines 55-60).

37. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a random number generator to secure assets to the *Angelo et al.*'s system in such a way that permitting access to the secured assets would include requesting and receiving the random number as taught by *Anderson, Jr.* One of ordinary skill in the art would have been motivated to perform such a modification in order to increase security (*Anderson, Jr.*, col. 7 line 55-60).

Art Unit: 2134

38. Claims 24 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Angelo et al. (U.S. Patent No. 6581162) in view of *Vogt et al. (U.S. Patent No. 6775776)*.

39. *Angelo et al.* teach a system including secure counters (*col. 4 line 58*).

40. *Angelo et al.* do not explicitly teach a monotonic counter, and wherein permitting access to secured assets includes requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter (*col. 7 line 66- col. 8 line 2*).

41. *Vogt et al.* teach monotonic counter (*Vogt et al., col. 7 line 56-col. 8 line 7*) and teach implicitly permitting access to secured assets include requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter.

42. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a monotonic counter wherein permitting access to secured assets included requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter as taught by *Vogt et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent a communication from being recorded and later played back to simulate a legitimate communication (*Vogt et al., col. 7 lines 64-66*).

43. Claims 31, 37 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Takahashi et al. (U.S. Patent No. 5615263)* in view of Official Notice.

44. As per claims 31, 37 and 50 Official Notice is taken that it is old and well-known to provide a predetermined response in lieu of data upon receipt of an access request to restricted assets.

45. Claims 10, 29 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Angelo et al.* (U.S. Patent No. 6581162) in view of *Colvin* (U.S. Patent No. 6044471).

46. *Angelo et al.* teach a timer as discussed in paragraph 10.

Angelo et al. do not teach measuring a time period in which the computer system is out of the secure operating mode in response to providing the control signal to the computer system to exit the secure operating mode and providing a control signal to the computer system to re-enter the secure operating mode in response to the time period in which the computer system is out of the secure operating mode exceeding a predetermined length of time.

47. *Colvin* implicitly teaches measuring a time period in which the computer system is out of the secure operating mode in response to providing the control signal to the computer system to exit the secure operating mode and providing a control signal to the computer system to re-enter the secure operating mode in response to the time period in which the computer system is out of the secure operating mode exceeding a predetermined length of time (*Colvin*, col. 2 lines 57-60).

48. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to measuring a time period in which the computer system is out of the secure operating mode in response to providing the control signal to the computer

system to exit the secure operating mode and providing a control signal to the computer system to re-enter the secure operating mode in response to the time period in which the computer system is out of the secure operating mode exceeding a predetermined length of time as taught by *Colvin*. One of ordinary skill in the art would have been motivated to perform such a modification in order to increase the level of system security (*Colvin*, col. 3 lines 20-27).

49. Claims 28, 5-8 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Angelo et al.* (U.S. Patent No. 5748888) in view of *Darago et al.* (U.S. Patent No. 6170014) and *Hunter et al.* (U.S. Patent No. 5920850).

50. *Angelo et al.* teach a system as discussed above and timers (col. 4 line 10). *Angelo et al.* also teaches an interrupt asserted by a timer (col. 5 lines 43-45).

51. *Angelo et al.* do not explicitly teach measuring a time period in which the computer system is in the secure operating mode; and providing a control signal to the computer system to exit the secure operating mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time.

52. *Darago et al.* teach time restricted secure transactions (col. 22 lines 34-38) and *Hunter et al.* teach a count down timer causing an output signal when a count down time has timed out (col. 8 lines 6-14).

53. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize the timer taught by *Angelo et al.* and measure a time period in which the computer system is in the secure operating mode; and providing a control

signal to the computer system to exit the secure operating mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time as taught by *Darago et al.* and *Hunter et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to make sure that the system is not left unattended such as when no input occurs for any specific time while in the secure mode.

54. Claims 5-8 are substantially equivalent to claim 28; therefore claims 5-8 are similarly rejected.

55. Claims 10 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Colvin* (U.S. Patent No. 6044471) in view of *Angelo et al.* (U.S. Patent No. 5748888) and in further view of *Darago et al.* (U.S. Patent No. 6170014) and *Hunter et al.* (U.S. Patent No. 5920850).

56. *Colvin et al.* teach requiring passwords while using software. *Colvin et al.* teach password being required periodically (*at a predetermined interval*).

57. *Colvin et al.* do not teach switching the computer between secure and non-secure operating modes. *Colvin et al.* also do not teach measuring a time period in which the computer system is out of the secure operating mode in response to providing the control signal to the computer system to exit the secure operating mode and providing a control signal to the computer system to re-enter the secure operating mode in response to the time period in which the computer system is out of the secure operating mode exceeding a predetermined length of time.

58. *Angelo et al.* teach a system operating in a secure and non-secure operating mode (where the secure mode is entered in order to prevent password spoofing) as discussed above and *Hunter et al.* teach a count down timer causing an output signal when a count down time has timed out (col. 8 lines 6-14).
59. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to measure a time period in which the computer system is out of the secure operating mode in response to providing the control signal to the computer system to exit the secure operating mode and providing a control signal to the computer system to re-enter the secure operating mode in response to the time period in which the computer system is out of the secure operating mode exceeding a predetermined length of time as taught by *Angelo et al.* and *Hunter et al.*'s. One of ordinary skill in the art would have been motivated to perform such a modification in order to enhance *Colvin et al.*'s invention by preventing password spoofing.
60. Claim 10 is substantially equivalent to claim 29; therefore claim 10 is similarly rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Signature

11/05/04

Date



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100